

PROTEGENDO SEU SERVIDOR SSH DE ATAQUES “BRUTE FORCE”

Diego M. Rodrigues (diego@drsolutions.com.br)

DenyHosts é um script escrito por Phil Schwartz para ajudar administradores de sistemas bloquear ataques de força bruta em seus servidores SSH. Ele monitora os arquivos de LOG do sistema (/var/log/secure no Redhat, /var/log/auth.log on Mandrake, etc...) e quando um ataque é detectado adiciona o IP do atacante no /etc/hosts.deny.

Quando executado pela primeira vez, o DenyHosts irá criar um diretório de trabalho para armazenar as informações coletadas dos arquivos de LOG em um formato que nós, humanos mortais, possamos ler, compreender e editar caso seja necessário.

O script possui uma grande variedade de configurações que podem ser exploradas, como por exemplo, configurar quantas tentativas inválidas devem ser consideradas um ataque, ou quantas tentativas erradas de usuários que não existem no seu sistema são aceitas... pode enviar emails com relatórios... essas configurações serão explicadas adiante no artigo.

PRÉ-REQUISITOS

Para que o DenyHosts funcione seu sshd deve estar configurado com suporte à TCP_WRAPPERS. Para realizar um teste e saber se no seu computador o sshd foi compilado dessa forma, faça o seguinte teste:

Logue-se na máquina como root:

```
[diego@marge ~]$ su -l
```

Agora altere o arquivo /etc/hosts.deny e acrescente a seguinte linha no final do arquivo:

```
$ sshd: 127.0.0.1
```

Usando o VI:

```
[root@marge ~]# vi /etc/hosts.deny
```

Seu arquivo deve ficar algo do tipo:

```
#
# hosts.deny      This file describes the names of the hosts which are
#                 *not* allowed to use the local INET services, as decided
#                 by the '/usr/sbin/tcpd' server.
$ sshd: 127.0.0.1
```

Agora tente fazer uma conexão ssh em localhost:

```
[root@marge ~]# ssh localhost
ssh_exchange_identification: Connection closed by remote host
[root@marge ~]#
```

Se você recebeu a mensagem com "Connection closed by remote host" quer dizer que está tudo Ok com o seu servidor ssh!

Altere novamente seu arquivo `/etc/hosts.deny` e remova a linha "`$ sshd: 127.0.0.1`" que você incluiu.

Outra coisa que precisa estar presente na sua máquina é o Python v2.3 ou superior. Execute o seguinte comando para saber qual versão você tem:

```
[root@marge ~]# rpm -q python
```

Caso você não possua o Python instalado, tente instar via `apt-get` (`apt-get install python`), `yum` (`yum install python`) ou use o RPM no CD da sua distribuição.

Na minha máquina (Fedora Core 4), eu tenho a versão 2.4

```
[root@marge ~]# rpm -q python
python-2.4.1-2
[root@marge ~]#
```

INSTALANDO

Faça download da última versão do DenyHosts na página oficial:

<http://denyhosts.sourceforge.net/>

Eu usei a versão 1.1.4, que era a mais recente quando estava escrevendo esse artigo.

Vamos então desempacotar o arquivo:

```
[root@marge ~]# tar xvfz DenyHosts-1.1.4.tar.gz
```

Eu particularmente gosto de manter o sistema organizado, portanto vou colocar o DenyHosts dentro do `/sbin`

```
[root@marge ~]# mv DenyHosts-1.1.4/ /sbin/DenyHosts
```

Vamos criar um arquivo de configuração baseado no arquivo de configuração exemplo:

```
[root@marge ~]# cd /sbin/DenyHosts/
[root@marge DenyHosts]# cp denyhosts.cfg-dist denyhosts.cfg
```

Agora vamos editar o arquivo de configuração:

```
[root@marge DenyHosts]# vi denyhosts.cfg
```

Configurações Básicas:

SECURE_LOG: Deve apontar para o seu arquivo de Logs.

```
SECURE_LOG = /var/log/secure
```

PURGE_DENY: Depois de quanto tempo o bloqueio para aquele IP é removido. No exemplo abaixo eu setei para 2 semanas:

```
PURGE_DENY = 2w
```

DENY_THRESHOLD_INVALID: Número de tentativas que um usuário inválido (não está no `/etc/passwd` deve fazer para que seja bloqueado). Exemplo:

```
DENY_THRESHOLD_INVALID = 5
```

DENY_THRESHOLD_INVALID: Número de tentativas que um usuário válido no sistema (está no `/etc/passwd` deve fazer para que seja bloqueado). Exemplo:

```
DENY_THRESHOLD_VALID = 10
```

DENY_THRESHOLD_ROOT: Número de tentativas que alguém pode fazer com senha de ROOT antes de ser bloqueado. Exemplo:

```
DENY_THRESHOLD_ROOT = 1
```

WORK_DIR: Diretório de trabalho do DenyHosts. Exemplo:

```
WORK_DIR = /usr/share/denyhosts/data
```

HOSTNAME_LOOKUP: Quando setado para "YES", todo IP reportado ao DenyHosts tentará ser resolvido.

```
HOSTNAME_LOOKUP=YES
```

Configurações Opcionais

ADMIN_EMAIL: Email que irá receber os relatórios de segurança.

```
ADMIN_EMAIL = diego@drsolutions.com.br
```

SMTP_*: Configura a conta de email que será usada para o envio dos emails de relatórios. Exemplo:

```
SMTP_HOST = smtp.drsolutions.com.br
```

```
SMTP_PORT = 25
```

```
SMTP_FROM = DenyHosts <diego@drsolutions.com.br>
```

```
SMTP_SUBJECT = DenyHosts Report
```

```
SMTP_USERNAME = diego
```

```
SMTP_PASSWORD = senha.aqui
```

Configurações do modo Daemon

DAEMON_LOG: Arquivo de LOG do DenyHosts.

```
DAEMON_LOG = /var/log/denyhosts
```

DAEMON_SLEEP: De quanto em quanto tempo o DenyHosts deve varrer o arquivo de logs do sistema. No exemplo abaixo deixamos 30s:

```
DAEMON_SLEEP = 30s
```

DAEMON_SLEEP: De quanto em quanto tempo o DenyHosts deve "expirar" as entradas velhas do arquivo HOSTS_DENY. Exmplo (configurei para 6 horas):

```
DAEMON_PURGE = 6h
```

EXECUTANDO

Para executar o DenyHosts em modo daemon, basta digitar /diretorioinstalado/denyhosts.py --daemon , por exemplo:

```
[root@marge DenyHosts]# /sbin/DenyHosts/denyhosts.py --daemon
```

Coloque esse comando no seu rc.local para que o DenyHosts seja executado automaticamente quando o computador for ligado:

```
[root@marge DenyHosts]# echo "/sbin/DenyHosts/denyhosts.py --daemon" >> /etc/rc.local
```

UM TESTE SIMPLES

Vamos tentar logar com o usuário "papainoel" (que não existe no meu sistema) no nosso servidor SSH:

```
[root@marge DenyHosts]# ssh papainoel@localhost  
papainoel@localhost's password:  
Permission denied, please try again.
```

Agora vamos ver se o DenyHosts detectou:

```
[root@marge DenyHosts]# cat /usr/share/denyhosts/data/users-invalid  
papainoel:2:Wed Jan 11 16:41:11 2006  
[root@marge DenyHosts]#
```

É isso aí.. tudo funcionando!

Abraços,
Diego M. Rodrigues
(diego@drsolutions.com.br)